

LISTING OF THE CLAIMS

1. (Currently amended) A method, comprising:
receiving, by an access point (AP) after distribution of a pairwise master key, a probe request;
defining an access point (AP) nonce of an AP; and
transmitting, by the AP, in response to a probe request, transmitting, from the AP, the AP nonce in a probe response including an AP nonce generated by the AP; and
receiving, by the AP, a pairwise master key request information element as a reassociate request from a user station that received the transmitted AP nonce, the pairwise master key request information element including the AP nonce, a user station nonce, and a message integrity code, wherein the message integrity code was computed using a message integrity code algorithm with a key confirmation key, the AP nonce, and the user station nonce, and wherein the key confirmation key was computed using a pseudo-random function algorithm with the pairwise master key, a media access control address of the AP, and a media access control address of the user station.
2. (Canceled)
3. (Currently amended) A method as claimed in claim 21, further comprising:
generating, by the AP, a pairwise master key response element based on the user station nonce and an additional message integrity code, the additional message integrity code being derived from the pairwise master key computed using the message integrity code algorithm with a key encryption key, the probe response, and the pairwise master key request information element, and wherein the key encryption key is computed using the pseudo random function algorithm with the pairwise master key, the media access control address of the AP, and the media access control address of the user station; and
transmitting, by the AP, the pairwise master response element as a reassociation response.

4. (Previously presented) A method as claimed in claim 3, further comprising communicating, by the AP, with the user station after the user station receives the reassociation response.

5. (Currently amended) A method, comprising:

transmitting, by a user station after distribution of a pairwise master key, a probe request to an access point (AP);

~~defining an AP nonce of the AP; and~~

receiving, by the user station, ~~the a probe response including an AP nonce transmitted from the AP in response to the probe request generated by the AP;~~

transmitting, by the user station, a pairwise master key request information element as a reassociate request to the AP, the pairwise master key request information element including the AP nonce, a user station nonce, and a message integrity code, wherein the message integrity code is computed using a message integrity code algorithm with a key confirmation key, the AP nonce, and the user station nonce, and wherein the key confirmation key is computed using a pseudo random function algorithm with the pairwise master key, a media access control address of the AP, and a media access control address of the user station.

6. (Canceled)

7. (Currently amended) A method as claimed in claim ~~65~~, further comprising:

~~_____receiving, by the user station, a pairwise master key response element from the AP, wherein the pairwise master key is a response element that is transmitted by the AP as a reassociation response and is based on the user station nonce and an additional message integrity code, the additional message integrity code being derived from the pairwise master key computed using the message integrity code algorithm with a key encryption key, the probe response, and the pairwise master key request information element, and wherein the key encryption key was computed using the pseudo random function algorithm with the pairwise master key, the media access control address of the AP, and the media access control address of the user station.~~

8. (Previously presented) A method as claimed in claim 7, further comprising communicating, by the user station, with the AP after receiving the reassociation response.

9. (Currently amended) An article of manufacture comprising a storage medium having stored thereon instructions that, when executed by a computing platform, result in an authenticated key exchange, by:

receiving, by an access point (AP) after distribution of a pairwise master key, a probe request;

defining an access point (AP) nonce of an AP;

transmitting, by the AP from the AP the AP nonce in a probe response in response to a the probe request, a probe response including an AP nonce generated by the AP; and

receiving, by the AP, a pairwise master key request information element as a reassociate request from a user station that received the transmitted AP nonce, the pairwise master key request information element including the AP nonce, a user station nonce, and a message integrity code, wherein the message integrity code was computed using a message integrity code algorithm with a key confirmation key, the AP nonce, and the user station nonce, and wherein the key confirmation key was computed using a pseudo random function algorithm with the pairwise master key, a media access control address of the AP, and a media access control address of the user station.

10. (Canceled)

11. (Currently amended) An article as claimed in claim 409, wherein the instructions, when executed, further result in an authenticated key exchange by:

generating, by the AP, a pairwise master key response element based on the user station nonce and an additional message integrity code, the additional message integrity code being derived from the pairwise master key computed using the message integrity code algorithm with a key encryption key, the probe response, and the pairwise master key request information element, and wherein the key encryption key is computed using the pseudo random function

algorithm with the pairwise master key, the media access control address of the AP, and the media access control address of the user station; and

transmitting, by the AP, the pairwise master response element as a reassociation response.

12. (Previously presented) An article as claimed in claim 11, wherein the instructions, when executed, further result in an authenticated key exchange by communicating, by the AP, with the user station after the user station receives the reassociation response.

13. (Currently amended) An article of manufacture comprising a storage medium having stored thereon instructions that, when executed by a computing platform, result in an authenticated key exchange, by:

transmitting, by a user station after distribution of a pairwise master key, a probe request to an access point (AP); and

receiving, by the user station, a probe response including an AP nonce transmitted from the AP in response to the probe request, wherein the AP nonce is defined as a nonce of the AP generated by the AP;

transmitting, by the user station, a pairwise master key request information element as a reassociate request, the pairwise master key request information element including the AP nonce, a user station nonce, and a message integrity code, wherein the message integrity code is computed using a message integrity code algorithm with a key confirmation key, the AP nonce, and the user station nonce, and wherein the key confirmation key is computed using a pseudo random function algorithm with the pairwise master key, a media access control address of the AP, and a media access control address of the user station.

14. (Canceled)

15. (Currently amended) An article as claimed in claim 14, wherein the instructions, when executed, further result in an authenticated key exchange by receiving, by the user station, a pairwise master key response element from the AP, wherein the pairwise master key is a

response element ~~that is transmitted by the AP as a reassociation response and is based on the user station nonce and an additional message integrity code, the additional message integrity code being derived from the pairwise master key computed using the message integrity code algorithm with a key encryption key, the probe response, and the pairwise master key request information element, and wherein the key encryption key is computed using the pseudo random function algorithm with the pairwise master key, the media access control address of the AP, and the media access control address of the user station.~~

16. (Previously presented) An article as claimed in claim 15, wherein the instructions, when executed, further result in an authenticated key exchange by communicating, by the user station, with the AP after receiving the reassociation response.

17. (Currently amended) An apparatus, comprising:

an omnidirectional antenna;

a transceiver coupled to said omnidirectional antenna; and

a baseband processor to:

generate a probe request to be transmitted to an access point (AP), and to receive a probe response including an AP nonce transmitted in response to the probe request, wherein the AP nonce is defined as a nonce of generated by the AP; and

generate a pairwise master key request information element including the AP nonce, a user station nonce, and a message integrity code, the message integrity code being computed using a message integrity code algorithm with a key confirmation key, the AP nonce, and the user station nonce, and wherein the key confirmation key is computed using a pseudo random function algorithm with the pairwise master key, a media access control address of the AP, and a media access control address of the user station.

18. (Canceled)

19. (Currently amended) An apparatus as claimed in claim 18, said baseband processor to receive a pairwise master key response element from the AP, wherein the pairwise master key

response element is transmitted by the AP as a reassociation response and is based on the ~~additional-user station~~ nonce and an additional message integrity code, the additional message integrity code being ~~derived from the pairwise master key~~ computed using the message integrity code algorithm with a key encryption key, the probe response, and the pairwise master key request information element, and wherein the key encryption key was computed using the pseudo random function algorithm with the pairwise master key, the media access control address of the AP, and the media access control address of the user station.

20. (Previously presented) An apparatus as claimed in claim 19, said baseband processor to establish communication with the AP after receiving the reassociation response.